



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

10/615,882

07/08/2003

Philip Michael Hawkes

030441

9835

23696

7590

11/14/2006

QUALCOMM INCORPORATED
5775 MOREHOUSE DR.
SAN DIEGO, CA 92121

EXAMINER

SIMITOSKI, MICHAEL J

ART UNIT

PAPER NUMBER

2134

DATE MAILED: 11/14/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

10/615,882

Applicant(s)

HAWKES ET AL.

Examiner

Michael J. Simitoski

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 15 August 2006.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-5, 8-16, 19-25, 28-34, 37-43, 46-52 and 55-63 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-5, 8-16, 19-25, 28-34, 37-43, 46-52 and 55-63 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 02 February 2004 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. The response of 8/15/2006 was received and considered.
2. Claims 1-5, 8-16, 19-25, 28-34, 37-43, 46-52 & 55-63 are pending.

Response to Arguments

3. Applicant's arguments with respect to claims 1-5, 8-16, 19-25, 28-34, 37-43, 46-52 & 55-63 have been considered but are moot in view of the new ground(s) of rejection.
4. The claimed invention has been amended to include that various keys are received over-the-air. However, as explained below, the claims are maintained as unpatentable over the prior art. Wasilewski is cited for teaching the use of a set top unit which generates it's own public key and therefore must distribute the key to service providers and Tsuria is cited for teaching the use of wireless communications, whose benefits are well known in the art of electronic communication for reducing the need for cables and allowing increased flexibility and mobility in data communications.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

6. Claims 1-5, 8-16, 19-25, 28-34, 37-43, 46-52 & 55-63 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent Re. 33,189 to Lee et al. (Lee) in view of U.S.

Patent 5,870,474 to Wasilewski et al. (**Wasilewski**) and U.S. Patent 6,424,947 to Tsuria et al. (**Tsuria**).

Regarding claims 1, 22, 40 & 58, Lee discloses distributing a key/user ID (col. 3, lines 28-42), receiving a secret key encrypted by the key/user ID (col. 4, lines 1-22), decrypting the secret key/ key by the key/user ID (col. 4, lines 1-22), receiving the access key/random number encrypted by the secret key/key (col. 4, lines 1-22) and decrypting the access key/random number by the secret key/key (col. 4, lines 1-22). Lee lacks a public key. However, Wasilewski teaches that in video distribution, the top key in the hierarchy of keys is a private key stored in a set top unit (col. 8, lines 44-47) where the second level key is encrypted with the public key which corresponds with the intended set top unit (col. 8, lines 39-41) because using a public key system obviates the need to securely transfer an endless hierarchy of keys (col. 8, lines 34-37) and allows multiple service providers to communicate with the set top unit (col. 10, lines 45-46). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Lee to utilize a public/private key pair as a replacement for the user ID and distribute a public key (to service providers) from the terminal (set top unit) and from a directory. One of ordinary skill in the art would have been motivated to perform such a modification because it obviates the need to securely transfer an endless hierarchy of keys and allows multiple service providers to communicate with the set top unit, as taught by Wasilewski (col. 8, lines 34-47 & col. 10, lines 45-46). As modified, Lee lacks distributing the public key over the air and receiving the secret key over the air. However, Tsuria teaches a system where a wireless subscriber unit receives television transmissions over the air (RF link) (col. 9, lines 35-48) to eliminate the need for a physical cable connection, as shown in Fig. 2 (#106 & #110).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Lee to use a wireless terminal and therefore, distribute the public key from the terminal (once it is generated, as taught by Wasilewski) over the air and to receive the secret key over the air (television communications). One of ordinary skill in the art would have been motivated to perform such a modification to gain the known benefits of wireless computing devices, such as the elimination of direct cable connections, as taught by Tsuria (col. 9, lines 35-48 & Fig. 2 #106 & #110).

Regarding claims 2, 10, 14, 20, 23, 29, 32, 38, 41, 47, 50, 56 & 59, Lee discloses the secret key being a registration key (col. 2, lines 41-51).

Regarding claims 3, 11, 15, 21, 24, 30, 33, 39, 42, 48, 51 & 57, Lee discloses the secret key being a temporary key/key of the month (col. 3, lines 28-42).

Regarding claims 4, 12 & 63, Lee discloses deriving a short key/PN sequence based on the access key/random number, receiving encrypted broadcast content/video and decrypting the encrypted broadcast content using the short key/PN sequence (col. 3, line 28 - col. 4, line 22).

Regarding claims 5, 25, 43 & 60, Lee discloses distributing a key/user ID (col. 3, lines 28-42), receiving the broadcast access key/key encrypted by the key/user ID and decrypting the broadcast access key/key by the private key/user ID (col. 4, lines 1-22). Lee lacks a public key. However, Wasilewski teaches that in video distribution, the top key in the hierarchy of keys is a private key stored in a set top unit (col. 8, lines 44-47) where the second level key is encrypted with the public key which corresponds with the intended set top unit (col. 8, lines 39-41) because using a public key system obviates the need to securely transfer an endless hierarchy of keys (col. 8, lines 34-37) and allows multiple service providers to communicate with the set top unit

Art Unit: 2134

(col. 10, lines 45-46). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Lee to utilize a public/private key pair as a replacement for the user ID and distribute a public key (to service providers) from the terminal (set top unit) and from a directory. One of ordinary skill in the art would have been motivated to perform such a modification because it obviates the need to securely transfer an endless hierarchy of keys and allows multiple service providers to communicate with the set top unit as taught by Wasilewski (col. 8, lines 34-47 & col. 10, lines 45-46). As modified, Lee lacks distributing the public key over the air and receiving the broadcast access key over the air. However, Tsuria teaches a system where a wireless subscriber unit receives television transmissions over the air (RF link) (col. 9, lines 35-48) to eliminate the need for a physical cable connection, as shown in Fig. 2 (#106 & #110). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Lee to use a wireless terminal and therefore, distribute the public key from the terminal (once it is generated, as taught by Wasilewski) over the air and to receive the broadcast access key over the air (television communications). One of ordinary skill in the art would have been motivated to perform such a modification to gain the known benefits of wireless computing devices, such as the elimination of direct cable connections, as taught by Tsuria (col. 9, lines 35-48 & Fig. 2 #106 & #110).

Regarding claims 8 & 61, Lee discloses deriving a short key/random number based on the access key/key, receiving encrypted broadcast content/video and decrypting the encrypted broadcast content/video using the short key/random number (col. 3, line 28 - col. 4, line 22).

Regarding claims 9, 28, 46 & 62, Lee discloses receiving a key/user ID corresponding to a private key/user ID (col. 3, lines 28-42), encrypting the secret key/key with the key/user ID (col. 3, lines 42-64), sending the encrypted secret key/key (col. 3, lines 1-22), receiving the access key/random number encrypted by the secret key/key (col. 4, lines 1-22) and decrypting the access key/random number by the secret key/key (col. 3, line 28 - col. 4, line 22). Lee lacks a public key. However, Wasilewski teaches that in video distribution, the top key in the hierarchy of keys is a private key stored in a set top unit (col. 8, lines 44-47) where the second level key is encrypted with the public key which corresponds with the intended set top unit (col. 8, lines 39-41) because using a public key system obviates the need to securely transfer an endless hierarchy of keys (col. 8, lines 34-37) and allows multiple service providers to communicate with the set top unit (col. 10, lines 45-46). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Lee to utilize a public/private key pair as a replacement for the user ID and distribute a public key (to service providers) from the terminal (set top unit) and from a directory. One of ordinary skill in the art would have been motivated to perform such a modification because it obviates the need to securely transfer an endless hierarchy of keys and allows multiple service providers to communicate with the set top unit as taught by Wasilewski (col. 8, lines 34-47 & col. 10, lines 45-46). As modified, Lee lacks receiving the public key over the air and sending the encrypted secret key over the air. However, Tsuria teaches a system where a wireless subscriber unit receives television transmissions over the air (RF link) (col. 9, lines 35-48) to eliminate the need for a physical cable connection, as shown in Fig. 2 (#106 & #110). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify

Art Unit: 2134

Lee to use a wireless terminal and therefore, receive the public key from the terminal (once it is generated, as taught by Wasilewski) over the air and to send the secret key over the air (television communications). One of ordinary skill in the art would have been motivated to perform such a modification to gain the known benefits of wireless computing devices, such as the elimination of direct cable connections, as taught by Tsuria (col. 9, lines 35-48 & Fig. 2 #106 & #110).

Regarding claims 13, 31 & 49, Lee discloses receiving a key/user ID (col. 3, lines 28-42), encrypting a secret key/key using the key/user ID (col. 3, lines 42-64), sending the encrypted secret key/key (col. 4, lines 1-5), encrypting the access key/random number using the secret key/key (col. 3, lines 42-64) and sending the encrypted access key/random number (col. 4, lines 1-22). Lee lacks a public key. However, Wasilewski teaches that in video distribution, the top key in the hierarchy of keys is a private key stored in a set top unit (col. 8, lines 44-47) where the second level key is encrypted with the public key which corresponds with the intended set top unit (col. 8, lines 39-41) because using a public key system obviates the need to securely transfer an endless hierarchy of keys (col. 8, lines 34-37) and allows multiple service providers to communicate with the set top unit (col. 10, lines 45-46). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Lee to utilize a public/private key pair as a replacement for the user ID and distribute a public key (to service providers) from the terminal (set top unit) and from a directory. One of ordinary skill in the art would have been motivated to perform such a modification because it obviates the need to securely transfer an endless hierarchy of keys and allows multiple service providers to communicate with the set top unit as taught by Wasilewski (col. 8, lines 34-47 & col. 10, lines

Art Unit: 2134

45-46). As modified, Lee lacks receiving the public key over the air and sending the encrypted secret key over the air. However, Tsuria teaches a system where a wireless subscriber unit receives television transmissions over the air (RF link) (col. 9, lines 35-48) to eliminate the need for a physical cable connection, as shown in Fig. 2 (#106 & #110). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Lee to use a wireless terminal and therefore, receive the public key from the terminal (once it is generated, as taught by Wasilewski) over the air and to send the secret key over the air (television communications). One of ordinary skill in the art would have been motivated to perform such a modification to gain the known benefits of wireless computing devices, such as the elimination of direct cable connections, as taught by Tsuria (col. 9, lines 35-48 & Fig. 2 #106 & #110).

Regarding claims 16, 34 & 52, Lee discloses receiving a key/user ID (col. 4, lines 1-22), encrypting the broadcast access key/key using the key/user ID (col. 3, lines 42-64) and sending the encrypted broadcast access key/key (col. 3, lines 42-64). Lee lacks a public key. However, Wasilewski teaches that in video distribution, the top key in the hierarchy of keys is a private key stored in a set top unit (col. 8, lines 44-47) where the second level key is encrypted with the public key which corresponds with the intended set top unit (col. 8, lines 39-41) because using a public key system obviates the need to securely transfer an endless hierarchy of keys (col. 8, lines 34-37) and allows multiple service providers to communicate with the set top unit (col. 10, lines 45-46). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Lee to utilize a public/private key pair as a replacement for the user ID and distribute a public key (to service providers) from the terminal (set top unit)

and from a directory. One of ordinary skill in the art would have been motivated to perform such a modification because it obviates the need to securely transfer an endless hierarchy of keys and allows multiple service providers to communicate with the set top unit as taught by Wasilewski (col. 8, lines 34-47 & col. 10, lines 45-46). As modified, Lee lacks receiving the public key over the air and sending the encrypted broadcast access key over the air. However, Tsuria teaches a system where a wireless subscriber unit receives television transmissions over the air (RF link) (col. 9, lines 35-48) to eliminate the need for a physical cable connection, as shown in Fig. 2 (#106 & #110). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Lee to use a wireless terminal and therefore, receive the public key from the terminal (once it is generated, as taught by Wasilewski) over the air and to send the encrypted broadcast access key over the air (television communications). One of ordinary skill in the art would have been motivated to perform such a modification to gain the known benefits of wireless computing devices, such as the elimination of direct cable connections, as taught by Tsuria (col. 9, lines 35-48 & Fig. 2 #106 & #110).

Regarding claims 19, 37 & 55, Lee discloses distributing a key/user ID corresponding to a private key/user ID (col. 3, lines 28-42), receiving a secret key/key (col. 3, lines 42-64) encrypted by the key/user ID (col. 3, lines 42-64), decrypting the secret key/key by the private key/user ID (col. 4, lines 1-22), encrypting the access key/random number by the secret key/key (col. 3, lines 42-64) and sending the encrypted access key/random number (col. 3, line 28 - col. 4, line 22). Lee lacks a public key. However, Wasilewski teaches that in video distribution, the top key in the hierarchy of keys is a private key stored in a set top unit (col. 8, lines 44-47) where the second level key is encrypted with the public key which corresponds with the intended set

Art Unit: 2134

top unit (col. 8, lines 39-41) because using a public key system obviates the need to securely transfer an endless hierarchy of keys (col. 8, lines 34-37) and allows multiple service providers to communicate with the set top unit (col. 10, lines 45-46). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Lee to utilize a public/private key pair as a replacement for the user ID and distribute a public key (to service providers) from the terminal (set top unit) and from a directory. One of ordinary skill in the art would have been motivated to perform such a modification because it obviates the need to securely transfer an endless hierarchy of keys and allows multiple service providers to communicate with the set top unit, as taught by Wasilewski (col. 8, lines 34-47 & col. 10, lines 45-46). As modified, Lee lacks distributing the public key over the air and receiving the secret key over the air. However, Tsuria teaches a system where a wireless subscriber unit receives television transmissions over the air (RF link) (col. 9, lines 35-48) to eliminate the need for a physical cable connection, as shown in Fig. 2 (#106 & #110). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Lee to use a wireless terminal and therefore, distribute the public key from the terminal (once it is generated, as taught by Wasilewski) over the air and to receive the secret key over the air (television communications). One of ordinary skill in the art would have been motivated to perform such a modification to gain the known benefits of wireless computing devices, such as the elimination of direct cable connections, as taught by Tsuria (col. 9, lines 35-48 & Fig. 2 #106 & #110).

Commensurate with the method description above, the means for distributing the public key correspond with the set top unit, as modified above, the means for receiving the public key

Art Unit: 2134

correspond with the headend and then service provider, as modified above, the means for receiving the secret key or broadcast encryption key correspond with the set top unit, as modified above, and the means for sending the secret key or broadcast access key correspond with the headend and service provider.

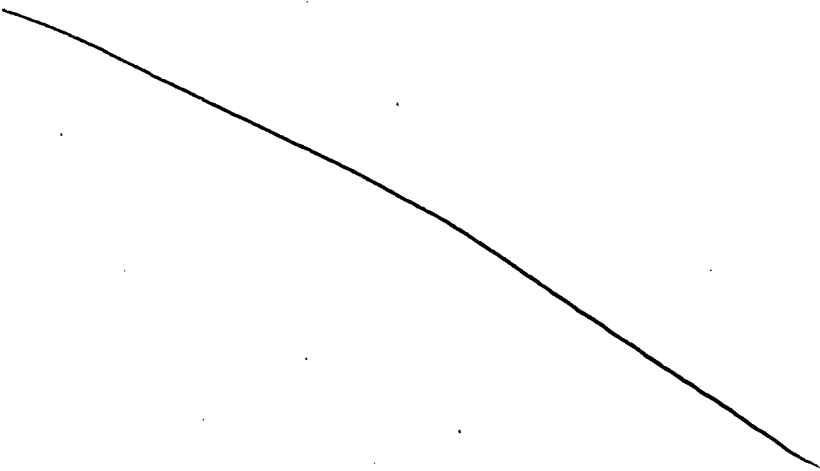
Conclusion

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. The Hylton and Voit references are cited for teaching wireless-network based video distribution.

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael J. Simitoski whose telephone number is (571) 272-3841. The examiner can normally be reached on Monday - Thursday, 6:45 a.m. - 4:15 p.m..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571) 272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

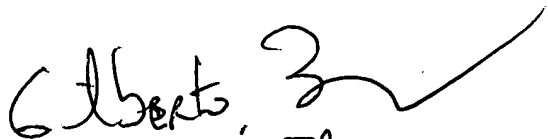


Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

MJS



November 6, 2006



GILBERTO BARRÓN JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100